(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2003－101529
(P2003－101529A)
(43)公開日　平成15年４月４日(2003.4.4)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04L 9/16		G06F 12/14	320B	5B017
G06F 12/14	320	G11B 20/10	H	5C052
G11B 20/10		H04N 5/76	A	5C053
H04N 5/76			Z	5C063
		7/173	630	5C064

審査請求 有　請求項の数８　ＯＬ　（全 11 頁）　最終頁に続く

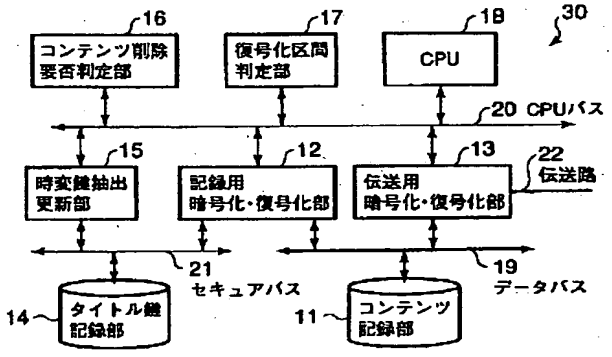
(21)出願番号　特願2001－287374(P2001－287374)
(22)出願日　平成13年９月20日(2001.9.20)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　大喜多　秀紀
神奈川県横浜市磯子区新杉田町８番地　株式会社東芝横浜事業所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　コンテンツ管理装置およびコンテンツ削除方法

(57)【要約】
【課題】　著作権保護機能により保護されたコンテンツをＭＯＶＥ処理もしくはＰＡＵＳＥ処理する際に、元のコンテンツを安全かつ効率的に削除する。
【解決手段】　タイトル鍵記録部１４はコンテンツ暗号化・復号化のためのタイトル鍵を記録する。記録用復号化・暗号化部１２はタイトル鍵記録部１４に記録された鍵を用いてコンテンツを復号化する。時変鍵抽出更新部１５はコンテンツ中の各ブロックを復号化する際生成された時変鍵を抽出する。又、時変鍵抽出更新部１５はタイトル鍵記録部１４が記録するタイトル鍵を、抽出された時変鍵で更新する。



1

【特許請求の範囲】

【請求項１】　コンテンツ暗号化・復号化のためのタイトル鍵を記録するタイトル鍵記録手段と、
前記タイトル鍵記録手段に記録された鍵を用いて前記コンテンツをブロック単位に復号化する復号化手段と、
前記復号化手段により前記コンテンツ中の各ブロックが復号化される際に生成される時変鍵を抽出する時変鍵抽出手段と、
前記タイトル鍵記録手段が記録するタイトル鍵を前記時変鍵抽出手段により抽出された時変鍵で更新する鍵更新手段、を有することを特徴とするコンテンツ管理装置。

【請求項２】　コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するコンテンツ削除要否判定手段を更に具備し、前記鍵更新手段は、前記コンテンツ削除要否判定手段によりコンテンツ削除が必要と判断された場合、前記タイトル鍵記録手段に記録された鍵の更新を行うことを特徴とする請求項１に記載のコンテンツ管理装置。

【請求項３】　前記特定区間分のコンテンツ復号化が完了したかどうかを判定する復号化区間判定手段を更に具備し、前記鍵更新手段は該復号化区間判定手段により前記特定区間の復号化が完了したと判定された場合、前記タイトル鍵記録手段に記録された鍵の更新を行うことを特徴とする請求項１に記載のコンテンツ管理装置。

【請求項４】　前記復号化手段は、あるブロックの暗号化・復号化に用いる時変鍵として少なくとも２つ以上前のブロックの暗号化・復号化により得られた時変鍵を用いることを特徴とする請求項１に記載のコンテンツ管理装置。

【請求項５】　前記復号化手段は、前記特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により導出された時変鍵を用いることを特徴とする請求項４に記載のコンテンツ管理装置。

【請求項６】　コンテンツの暗号化・復号化のためのタイトル鍵をタイトル鍵記録領域に記録するステップと、
タイトル鍵記録領域に記録された鍵を用いて前記コンテンツを復号化するステップと、
コンテンツ復号化の際生成される時変鍵を抽出するステップと、
前記タイトル鍵記録領域に記録されたタイトル鍵を前記時変鍵で更新するステップ、を有するコンテンツ削除方法。

【請求項７】　コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するステップと、
前記コンテンツ削除が必要と判断された場合、前記タイトル鍵領域の更新を行うステップを有することを特徴とする請求項６に記載のコンテンツ削除方法。

【請求項８】　特定区間分のコンテンツ復号化が完了したかどうかを判定するステップと、
前記特定区間の復号化が完了した場合、タイトル鍵領域の更新を行うステップとを有することを特徴とする請求項６に記載のコンテンツ削除方法。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は放送局側から配信されたコンテンツに対してＭＯＶＥ処理・ＰＡＵＳＥ処理を行う場合のコンテンツ削除方法に関する。

【０００２】

【従来の技術】著作権保護機能により保護されたコンテンツをＭＯＶＥ処理もしくはＰＡＵＳＥ処理する場合、著作権保護機能により定められたルールに従い、伝送もしくは記録後特定時間経過したコンテンツを装置から順次削除していく必要がある。

【０００３】ＭＯＶＥ処理は、Ｃｏｐｙ　Ｏｎｃｅコンテンツ（１回だけ記録を許されたコンテンツ）に対するコンテンツ移動処理である。Ｃｏｐｙ　Ｏｎｃｅコンテンツは記録が１回しか許可されていないため、他の記録媒体へのコピーは許可されていない。しかしコンテンツを例えば受信器の記録部に記録した後、該コンテンツの削除を条件に、他の記録先機器へ記録することが許されている。

【０００４】ＰＡＵＳＥ処理は、Ｃｏｐｙ　Ｎｅｖｅｒコンテンツ（記録が許可されていないコンテンツ）に対するタイムシフト視聴処理である。タイムシフト視聴は、放送中のコンテンツに対して一時停止やプレイバック再生を行う機能であり、コンテンツ視聴時のコーヒーブレイクやトイレ休憩（一時停止）やスポーツ中継などでの決定的瞬間のインスタントリプレイ（プレイバック再生）を提供できる。ＰＡＵＳＥ処理ではコンテンツを一定時間後削除することを条件に、例えば受信器の記録部に記録することが許されている。

【０００５】

【発明が解決しようとする課題】ＭＯＶＥ処理もしくはＰＡＵＳＥ処理においてコンテンツを削除する方法として、従来以下のようないくつかの方式が考えられる。

【０００６】まず第１の方式として、コンテンツデータそのものを削除していく方式が考えられる。しかし一般にコンテンツは膨大なデータ量がある。例えば通常のＶＨＳ並みの画質の映像コンテンツの場合で約５Ｍｂｐｓ（Ｍｅｇａ　ｂｉｔ　ｐｅｒｓｅｃｏｎｄ）程度、ハイビジョン画質の映像コンテンツで約２８Ｍｂｐｓ程度のデータ量がある。このような大量データの削除をＭＯＶＥ・ＰＡＵＳＥ処理と同時に行うことは負荷の大きい処理であり現実的でない。

【０００７】第２の方式として、コンテンツそのものを削除する代わりに、記録されたコンテンツを復号化不可能とするため、コンテンツの復号化に用いるタイトル鍵を消去する方式が考えられる。しかし、通常コンテンツ１つに対してタイトル鍵は１つであり、例えばＭＯＶＥ処理中の障害によるクラッシュ時に、コンテンツが送受

信側の双方に存在する、もしくは双方から消失するという事態が生じない様、コンテンツを伝送し終えるまで、タイトル鍵の削除・伝送が行えない。

【０００８】このため送信側ではコンテンツを送信分のみを削除するということができず、受信側ではコンテンツをすべて受信するまで復号化ができないという問題が生じる。このような問題のためコンテンツが映像ストリームや音声ストリームの場合など、伝送中にコンテンツを復号化してリアルタイムで再生・伝送・消去する必要がある場合に、この方式は適用できない。

【０００９】第３の方式として、コンテンツを複数の領域に分割し、それぞれを別のタイトル鍵で暗号化し、コンテンツの削除が必要になった場合、対応するタイトル鍵を順に削除していく方式が考えられる。当該方式はコンテンツが映像ストリームの場合に対しても有効であるが、コンテンツを細かく分割した場合、管理するタイトル鍵が膨大になるという問題がある。例えばコンテンツをフレーム単位に分割したとすると、１時間の映像コンテンツに対して１０万以上のタイトル鍵を管理する必要が生じる。

【００１０】タイトル鍵はコンテンツの著作権保護のため機密にする必要があり、通常のシステムからはアクセスできない保護領域で管理する必要がある。機密性を確保する必要のある保護領域を大量に準備することは現実的ではなく、当該方式によるコンテンツ削除をＭＯＶＥ処理やＰＡＵＳＥ処理に対して適用することは事実上困難である。

【００１１】本発明は上記の問題点に鑑み、著作権保護機能により保護されたコンテンツをＭＯＶＥ処理もしくはＰＡＵＳＥ処理する際に、元のコンテンツを安全かつ効率的に消去することを目的としている。

【００１２】

【課題を解決するための手段】上記目的を達成するために本発明は、コンテンツ暗号化・復号化のためのタイトル鍵を記録するタイトル鍵記録手段と、前記タイトル鍵記録手段に記録された鍵を用いて前記コンテンツをブロック単位に復号化する復号化手段と、前記復号化手段により前記コンテンツ中の各ブロックが復号化される際に生成される時変鍵を抽出する時変鍵抽出手段と、前記タイトル鍵記録手段が記録するタイトル鍵を前記時変鍵抽出手段により抽出された時変鍵で更新する鍵更新手段を有する。

【００１３】これにより、ＨＤＤ、ＤＶＤもしくはＳＤカードなどＣＰＲＭにおけるＣ－ＣＢＣ暗号などを用いて復号化したコンテンツを復号化が完了したものから順に効率的に削除することができる。

【００１４】更に本発明は、コンテンツに付加された著作権保護情報を基にコンテンツ削除の要否を判定するコンテンツ削除要否判定手段を具備し、前記鍵更新手段は、前記コンテンツ削除要否判定手段によりコンテンツ削除が必要と判断された場合、前記タイトル鍵領域の更新を行う。これにより、コンテンツ削除処理を、ＭＯＶＥ処理・ＰＡＵＳＥ処理などコンテンツ削除が必要な場合に適切に呼び出すことが出来る。

【００１５】又本発明は、前記特定区間分のコンテンツ復号化が完了したかどうかを判定する復号化区間判定手段を更に具備し、前記鍵更新手段は特定区間の復号化が完了した場合、前記タイトル鍵領域の更新を行う。

【００１６】これにより、タイトル鍵の更新（すなわちコンテンツの削除）を、ＩＥＥＥ１３９４パケット単位や、ＭＰＥＧ２のフレーム、ＧＯＰ単位などまとまった単位で行うことが出来、必要以上に頻繁にタイトル鍵を更新することによる処理効率の低下を防ぐことが出来る。

【００１７】又本発明は、あるブロックの暗号化・復号化に用いる時変鍵として、少なくとも２つ以上前のブロックの暗号化・復号化により得られた時変鍵を用いる。例えば、前記特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により導出された時変鍵を用いる。これにより、特殊再生やコンテンツのサーチを行う際、処理に必要な時変鍵を高速に生成が出来る。

【００１８】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態について詳細に説明する。図１は本発明に係るコンテンツ管理装置の構成の一実施形態を示すブロック図である。

【００１９】本発明のコンテンツ管理装置３０は、コンテンツ伝送を行うデータバス１９、制御情報をやり取りするＣＰＵバス２０、タイトル鍵や時変鍵を安全にやりとりするセキュアバス２１の３つのバスを用いて構成されている。

【００２０】コンテンツ記録部１１はコンテンツを記録あるいは一時蓄積する。記録用暗号化・復号化部１２はコンテンツに付加された著作権保護情報に基づき、コンテンツの暗号化・復号化を行う。記録用暗号化・復号化の具体例としてはＣＰＲＭ（Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉｏｎ　ｆｏｒ　Ｒｅｃｏｒｄａｂｌｅ　Ｍｅｄｉａ）などがある。

【００２１】コンテンツ記録部１１に記録された情報は、記録用暗号化・復号化部１２を通じて復号化され、データバス１９を介して伝送用暗号化・復号化部１３に転送される。伝送用暗号化・復号化部１３では受け取ったコンテンツを伝送用に暗号化し伝送路２２に流す。伝送路の具体例としてはＩＥＥＥ（Ｔｈｅ　Ｉｎｓｔｉｔｕｅ　ｏｆ　Ｅｌｅｃｔｉｒｃａｌ　ａｎｄ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｅｎｇｉｎｅｅｒｓ，Ｉｎｃ．）で規格化されているＩＥＥＥ　ｓｔｄ．１３９４－１９９５（ＩＥＥＥ１３９４）などがある。伝送用暗号化・復号化の具体例としては、ＤＴＣＰ（Ｄｉｇｉｔａｌ　Ｔｒａｎｍｉｓｓｏｎ　Ｃｏｎｔｅｎｔ　Ｐｒｏｔｅｃｔｉ

5

ｏｎ）などがある。

【００２２】記録用暗号化・復号化部１２は、セキュアバス２１を介してタイトル鍵記録部１４からタイトル鍵情報を受け取り、当該タイトル鍵を用いてコンテンツの暗号化・復号化を行う。タイトル鍵記録部１４は、不正アクセスを防ぐため通常の方法では読み出せない保護領域である。つまりタイトル鍵記録部１４は、ＣＰＵバス２０から直接アクセスすることはできず、記録用暗号化・復号化部１２とタイトル鍵記録部１４との認証処理を介してアクセス可能である。

【００２３】コンテンツ削除要否判定部１６はコンテンツに付与された著作権保護情報および現在の実行状態に基づきコンテンツ削除の要否を判定する。実行状態の具体例としてはＭＯＶＥ処理中もしくはＰＡＵＳＥ処理中などがある。時変鍵抽出更新部１５は、記録用暗号化・復号化部１２から暗号化・復号化の際生成する時変鍵（後述される）を抽出し、コンテンツ削除要否判定部１６の判定結果に応じて、コンテンツ削除の必要があればタイトル鍵記録部１４のタイトル鍵を、抽出した時変鍵により更新する。復号化区間判定部１７は特定区間の復号化が完了したかどうかを判定する。ＣＰＵ１８は本発明に従ってコンテンツ管理装置３０を総合的に制御する。

【００２４】図２はコンテンツに付与される著作権保護情報の一例を示す。「００」が付されたコンテンツはＣｏｐｙ　Ｆｒｅｅコンテンツであって、コピーを自由に行うことができる。「１０」が付されたコンテンツはＣｏｐｙ　Ｏｎｃｅコンテンツであって、コピーが１度だけ許可されている。Ｃｏｐｙ　Ｏｎｃｅコンテンツを記録媒体にコピーした場合、該著作権保護情報は「０１」に書き換えられ、以後のコピーが禁止される。「１１」が付されたコンテンツはＣｏｐｙ　Ｎｅｖｅｒコンテンツであって、コピーは禁止されている。

【００２５】図３は著作権保護のかかったコンテンツに対するＭＯＶＥ・ＰＡＵＳＥ処理の概要を示す図である。

【００２６】ＰＶＲ（Ｐｅｒｓｏｎａｌ　Ｖｉｄｅｏ　Ｒｅｃｏｒｄｅｒ）３１はコンテンツ管理装置３０を具備する装置の一具体例であり、ＨＤＤを内蔵しコンテンツを記録あるいは一時蓄積する機能を持つ。表示装置３２はテレビジョンなどに代表される機器で、デジタルもしはくアナログ映像を画面に表示する機能を持つ。記録装置３３はＤＶＨＳやＡＶ－ＨＤＤ，ＤＶＤなどに代表される機器で、映像の記録機能を持つ。ＰＶＲ３１は必要に応じてＭＯＶＥ処理もしくはＰＡＵＳＥ処理を行う。

【００２７】ＭＯＶＥ処理は、Ｃｏｐｙ　Ｏｎｃｅコンテンツに対するコンテンツ移動処理であるため、他の記録媒体へのコピー（ダビング）は許可されていない。しかしコンテンツをコンテンツ記録部１１のような受信器

6

の記録媒体に記録した後、該コンテンツの削除を条件に、他の記録先機器へ移動することが許されている。ＭＯＶＥ処理は、このようなコンテンツ移動処理を示す。

【００２８】ＭＯＶＥ処理では著作権保護に関する規定上、コンテンツの移動途中に障害が発生したとしても、送信元であるＰＶＲと受信先である記録装置に同一コンテンツが重複して存在することのないよう適切に制御されなければならない。また、１台のＰＶＲ３１の出力を複数台の記録機器で記録する操作は、コンテンツの複製を作成する操作となるためＭＯＶＥ処理では許可されていない。

【００２９】Ｃｏｐｙ　Ｎｅｖｅｒコンテンツは記録媒体への記録は許可されていないが、ＰＡＵＳＥ処理では記録時間に制限を設けることにより、コンテンツ記録部１１のような記録媒体への一時蓄積を許可し、一時停止やプレイバック再生を可能としている。制限時間の具体例としては、９０分や１日あるいは１週間などがある。一時蓄積したコンテンツは制限時間経過後削除する必要がある。

【００３０】ＰＡＵＳＥ処理は、ＤＴＣＰ規格ではＲＥＴＥＮＳＩＯＮ処理とも呼ばれており、処理に関する名称は本発明の限りではない。また、ＰＡＵＳＥ処理を、Ｃｏｐｙ　Ｏｎｃｅコンテンツに対して適用することも可能である。

【００３１】図４は、ＭＯＶＥ処理を具体的に説明する図である。

【００３２】コンテンツはＩＥＥＥ１３９４などのセキュアな伝送路２２を経由して、ＰＶＲ３１等の送信側機器から記録装置３３等の受信側機器に伝送される。送信側機器では送信済みのコンテンツを適切な手段で削除する必要がある。

【００３３】図５はＰＡＵＳＥ処理を具体的に説明する図である。

【００３４】矩形は記録領域を模式的に表したものである。記録位置は記録領域を左から右へ移動し、記録位置の左側はコンテンツが記録されている領域を表す。再生位置は記録位置より左側の制限時間内で自由に移動させることが出来る。記録してから制限時間を超過したコンテンツ（例えば記録後９０分経過したコンテンツ）は順次削除していく。

【００３５】図６は従来におけるコンテンツを削除する第１の方式を示した図である。

【００３６】当該方式では、コンテンツデータそのものを削除していく（例えば各データを「００」に書き換える）。しかし一般にコンテンツは膨大なデータ量がある。例えば通常のＶＨＳ並みの画質の映像コンテンツの場合で約５Ｍｂｐｓ（Ｍｅｇａｂｉｔ　ｐｅｒ　ｓｅｃｏｎｄ）程度、ハイビジョン画質の映像コンテンツで約２８Ｍｂｐｓ程度のデータ量がある。このような大量データの削除をＭＯＶＥあるいはＰＡＵＳＥ処理と同時に

行うことは負荷の大きい処理であり現実的でない。

【００３７】図７は従来におけるコンテンツを削除する第２の方式を示した図である。

【００３８】当該方式では、コンテンツそのものを削除する代わりに、コンテンツの復号化に用いるタイトル鍵を消去する。タイトル鍵を消去することにより、暗号化されたコンテンツを復号化することは不可能となり、結果的にコンテンツそのものを削除するのと同じ効果が得られる。タイトル鍵は通常５４ｂｉｔや１２８ｂｉｔなどのサイズでありコンテンツそのものの削除と比較して処理も容易である。当該方式はコンテンツが暗号化ファイルの場合など、コンテンツをすべて転送してから復号化のための鍵を送付する処理方式に対して有効である。

【００３９】しかし当該方式では、通常コンテンツ１つに対してタイトル鍵は１つであり、送信側ではコンテンツを送信し終えるまでタイトル鍵の削除が行えず、受信側ではコンテンツをすべて受信するまで復号化ができないという問題が生じる。このためコンテンツが映像ストリームや音声ストリームの場合など、伝送中にコンテンツを復号化してリアルタイムで削除する必要がある場合には適用できない。

【００４０】図８は従来におけるコンテンツを削除する第３の方式を示した図である。

【００４１】当該方式では、コンテンツを複数の領域に分割し、それぞれを別のタイトル鍵で暗号化する。そしてコンテンツの削除が必要になった場合、対応するタイトル鍵を順に削除していく方式をとる。当該方式はコンテンツが映像ストリームの場合に対しても有効であるが、コンテンツを細かく分割した場合、管理するタイトル鍵が膨大になるという問題がある。例えばコンテンツをフレーム単位に分割したとすると、１時間の映像コンテンツに対して１０万以上のタイトル鍵を準備し管理する必要が生じる。タイトル鍵はコンテンツの著作権保護のため機密にする必要があり、通常のシステムからはアクセスできない保護領域で管理する必要がある。機密性を確保する必要のある保護領域を大量に準備することは現実的ではなく、当該方式によるコンテンツ削除をＭＯＶＥ処理やＰＡＵＳＥ処理に対して適用することは事実上困難である。

【００４２】図９は上記問題点を鑑みて発明されたものであり、本方式におけるコンテンツを削除する方式の概略を示した図である。本方式では、コンテンツ復号化の際使用される時変鍵を抽出し、タイトル鍵領域の元のタイトル鍵を、抽出した当該時変鍵で順次上書きする方式をとる。これにより更新した時変鍵より前のコンテンツの復号化を不可能とする。

【００４３】図１０はコンテンツ暗号化方式の一例を示す。ここでは暗号化方式としてＣ－ＣＢＣ（Ｃｏｎｖｅｒｔｅｄ　Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ）を用いた暗号化処理について示す。Ｃ－ＣＢＣでコンテンツを暗号化する際、暗号化に用いる暗号鍵の推定を困難にし暗号強度を高めるため、処理途中で暗号鍵を変更する時変鍵方式という処理方式を用いる。ここで暗号鍵はタイトル鍵と同義である。この時変鍵は元の暗号鍵と平文コンテンツから計算により求めることができる。計算には逆演算の困難な一方向性関数を用いる。これにより暗号化コンテンツから平文コンテンツや暗号鍵を推定することを困難とし暗号強度を高めている。

【００４４】図１０では、コンテンツをブロック単位に分割した上で、まずタイトル鍵と最初のブロックを暗号化する。この暗号化の際導出された時変鍵を用いて第２のブロックを暗号化する。以下当該処理を各ブロックに順次適用することでコンテンツを暗号化する。

【００４５】図１１は図１０で示した暗号化方式により暗号化されたコンテンツを復号化する処理を示した図である。この復号化処理は、図１０で説明した暗号化処理とは逆の手順となり、タイトル鍵もしくはその時変鍵と暗号化コンテンツから平文コンテンツへの復号化を順次行っていく。

【００４６】以下、本発明におけるＭＯＶＥ・ＰＡＵＳＥ処理におけるコンテンツ削除方法について詳細に示す。

【００４７】図１２は本発明に係るコンテンツ復号化の際に行われるコンテンツ削除処理の第１の実施形態について示した図である。本方式では、コンテンツ復号化の際導出された時変鍵を抽出し、抽出された時変鍵で元のタイトル鍵を更新する処理を追加したことに特徴がある。

【００４８】記録用暗号化・復号化部１２は先ずブロックＢ１をタイトル鍵を用いて復号化する。このタイトル鍵はＰＶＲ３１が各コンテンツ毎に予め持っている値であり、タイトル鍵記録部１４内のタイトル鍵領域１４ａに記録されている。時変鍵抽出更新部１５は最初のブロックＢ１の復号化の際に時変鍵１を抽出する。また時変鍵抽出更新部１５は時点ｔ１において、タイトル鍵領域１４ａに格納されているタイトル鍵を時変鍵１で上書き、すなわち書き換える。

【００４９】次に記録用暗号化・復号化部１２は時変鍵１を用いてブロックＢ２を復号化する。時変鍵抽出更新部１５は２番目のブロックＢ２の復号化の際に時変鍵２を抽出し、時点ｔ２において時変鍵１を時変鍵２で上書きする。以後、時変鍵３、時変鍵４…という手順で、時変鍵抽出更新部１５はタイトル鍵領域１４ａの鍵を順次上書きしていく。

【００５０】このようにブロック単位の復号化の際得られた時変鍵でタイトル鍵領域１４ａを順次上書きしていくことで、上書きした時変鍵を用いて復号化されるブロックより前のブロックの復号化が不可能となり、コンテンツそのものを削除した場合と同一の結果が得られる。

【００５１】図１３は本方式におけるコンテンツ削除方

式を適用した場合のＭＯＶＥ処理において、処理中に障害が発生した場合の動作を示した図である。

【００５２】図１３では、ブロックＢ３を時変鍵Ｊｋ２で復号後、得られた時変鍵Ｊｋ３でタイトル鍵領域１４ａを上書きした後、障害が発生した場合を想定している。障害の具体例としては、停電による電源クラッシュや故障または不注意により伝送ケーブル抜き等が考えられる。この時すでに転送済みのコンテンツ（ブロックＢ１からＢ３）は消去済みもしくは２度と復号化できない状態でなければならない。

【００５３】本方式によるコンテンツ削除方法を適用したＭＯＶＥ処理では、障害発生時点でタイトル鍵領域１４ａはＪｋ３に書き換えられており、元のタイトル鍵Ｔｋとそこから導出される時変鍵Ｊｋ１およびＪｋ２は２度と得ることができない。このためブロックＢ１～Ｂ３のコンテンツは復号化不可能となり、事実上コンテンツが削除されたと同様の結果が得られる。

【００５４】障害発生後、処理を再開する場合、タイトル鍵領域１４ａのＪｋ３を用いてブロックＢ４を復号化し、該復号化の際に導出されるＪｋ４を用いてブロックＢ５を復号化し、以後同様に残りのコンテンツを復号化して伝送することが出来る。

【００５５】図１４は本方式によるコンテンツ削除方式を用いたＭＯＶＥ処理におけるタイトル鍵上書きのタイミングについて示した図である。

【００５６】ＭＯＶＥ処理においては、前述したようにコンテンツの各ブロックの復号化時点で抽出された時変鍵を、タイトル鍵領域に順次上書きしていく。これにより、送信分のコンテンツ削除を保証できる。

【００５７】図１５は本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第１の具体例について示した図である。

【００５８】ＰＡＵＳＥ処理においては記録時から制限時間（例えば９０分）経過したコンテンツを順次削除していく必要がある。第１の具体例では、図中再生位置Ｐ１で示される再生のためのコンテンツ復号化とは別に、位置Ｐ２に示すように記録時から制限時間分前のコンテンツを並列に復号化処理し、当該復号化処理で得られた時変鍵をタイトル鍵領域１４ａに上書きする。尚、再生のためのコンテンツ復号化の際に得られる時変鍵は保存しない。

【００５９】図１６は本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第２の具体例について示した図である。

【００６０】第２の具体例ではタイムシフト再生の時点で得られた時変鍵をタイトル鍵記憶部１４の一時保存領域１４ｂに一時的に保存しておき、制限時間になった時点で順次上書きしていく。これは再生位置と制限時間の間隔が短い場合やコンテンツ分割の間隔が大きい場合など記録すべき時変鍵の数が少ない場合に有効である。この時変鍵の一時保存領域１４ｂはタイトル鍵領域１４ａ同様、セキュアな領域に保護される必要がある。なお本実施形態では一時保存する時変鍵を制限時間までとしているが、インスタントリプレイが例えば数分など短時間であり、制限時間分再生位置を戻す必要がないなどの条件を満たせば、再生位置から例えば５分前まで保存するなど、保存する時変鍵の数を削減してもよく、時変鍵の保存期間は制限時間内で自由に設定できる。

【００６１】図１７は、本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第３の具体例について示した図である。

【００６２】第３の具体例ではタイムシフト再生の時点で得られた時変鍵を直接タイトル鍵領域に上書きする。これはコンテンツの一時停止のみをサポートし、インスタントプレイなど同一コンテンツを２度再生する必要が無い場合に有効である。

【００６３】図１８は本発明に係るコンテンツ削除の第２の実施形態を示した図である。

【００６４】図１８ではコンテンツ復号化の際得られた時変鍵を逐次タイトル鍵領域に上書きするのではなく、特定区間の復号化を完了するごとにタイトル鍵の上書きを行う。具体的にはＭＯＶＥ処理やＰＡＵＳＥ処理で要求される最小消去単位や、表示や伝送の単位など意味のある復号化が可能な最小単位が、暗号化・復号化に用いるブロックより大きい場合に有効である。復号化特定区間の具体例としてはＭＰＥＧにおけるフレーム単位・ＧＯＰ単位やＭＰＥＧ２－ＴＳにおけるＰＥＳ単位、ＩＥＥＥ１３９４におけるＩｓｏｃｈｒｏｎｏｕｓ Ｓｔｒｅａｍパケット単位、特定の時間単位などがある。特定区間は固定長である必要は無く、あるルールに従い区間の特定が可能であればよい。これによりタイトル鍵の上書き回数が削減され処理の効率化が図れる。

【００６５】図１９は本実施形態によるコンテンツ復号化処理時におけるコンテンツ削除方法を示すフローチャートである。

【００６６】ステップＳ０１で記録用暗号化・復号化部１２はタイトル鍵領域１４ａからタイトル鍵を取得する。ステップＳ０２で暗号化コンテンツから１ブロック読み込む。ステップＳ０３でタイトル鍵もしくは時変鍵を用いて１ブロックの暗号化コンテンツを復号化する。ステップＳ０４で時変鍵抽出更新部１５はステップＳ０３の復号化により導出された新しい時変鍵を抽出する。ステップＳ０５でコンテンツ削除要否判定部１６は現在の処理がＭＯＶＥ処理もしくはＰＳＵＳＥ処理であることを判定し、ＭＯＶＥ処理もしくはＰＡＵＳＥ処理であれば（コンテンツ削除の必要があれば）ステップＳ０６へ進み、そうでない場合はステップＳ０８に進む。ステ

ップＳ０６で復号化区間判定部１７は特定区間の復号化が完了したかどうかを判定し、完了していればステップＳ０７へ、完了していなければステップＳ０８へ進む。ステップＳ０７で時変鍵抽出更新部１５はタイトル鍵領域１４ａを新しい時変鍵で更新する。ステップＳ０８でＣＰＵ１８はコンテンツの全ブロックを復号化したか判定し、未復号化コンテンツが存在すればステップＳ０２に戻って処理を継続し、全てのブロックを復号化していれば終了する。

【００６７】図２０は本方式に係るコンテンツ削除の別の具体例を示した図である。

【００６８】図２０では特定区間の最後のブロックの復号化の際、特定区間の最初のブロックの復号化の際に使用した時変鍵を使用する。つまり、特定区間の最初のブロックを例えば時変鍵ｊｋｎを用いて復号化した場合、該特定区間の最後のブロックも時変鍵ｊｋｎを用いて復号化する。このとき時変鍵ｊｋｎ＋１が抽出される。次の特定区間の最初のブロック及び最後のブロックは時変鍵ｊｋｎ＋１を用いて復号化する。従って、特定区間の最後のブロックの復号化の際、前ブロックの最後の復号化により抽出された時変鍵を用いる。これにより複数区間をまたがる場合の時変鍵の導出を高速に行うことができる。これは、特定倍速再生などの特殊再生や巻戻し後の再生の際効果がある。

【００６９】なお本実施例では最後のブロックの復号化に最初のブロックの復号化に用いた時変鍵を適用した例を示したが、これは一般に後半のブロックの復号化の際に直前より前のブロックの復号化の際得られた時変鍵を適用すれば処理を効率化できる。ブロック復号化とそれに用いる時変鍵の組み合わせは本実施例の限りではない。

【００７０】図２１は図２０で示したコンテンツ削除方式を用いた場合における特殊再生およびサーチの動作を示す図である。

【００７１】図２１（ａ）は倍速再生を示す図、図２１（ｂ）はサーチ動作を示す図である。倍速再生領域及びサーチ領域における斜線領域は１画像フレームを示す。又、斜線で示された領域は全ブロックを復号化した領域、空白領域は特定区間の最後のブロックのみを復号化した領域である。

【００７２】通常の復号化処理では先頭からすべてのブロックを復号化しなければ特定位置の時変鍵は得られないが、図２０に示すコンテンツ削除方式を用いた場合、特殊再生やサーチの際に時変鍵を再計算する場合でも、特定ブロックの最後のみ復号化すればよいため、高速に所定位置の時変鍵を得ることが出来る。

【００７３】次に図２２、図２３を用いて、本発明を用いたコンテンツ削除方法に係る第３の実施形態について説明する。

【００７４】図２２は、従来におけるコンテンツ削除方法に関する別の具体例を示す図である。

【００７５】コンテンツを暗号化する際、コンテンツすべてを連続して暗号化するのではなく、特定の単位で処理を一旦リセットし、はじめから暗号化の処理を行う場合がある。例えばＳＤ（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌ）カードでは図２２に示すように暗号化を音声フレーム単位に行う。このように各復号化の際に同一のタイトル鍵Ｔｋ１を用いるため、最終フレームを復号化完了するまでタイトル鍵Ｔｋ１を削除することができない。

【００７６】図２３は上記のような暗号化が適用された場合におけるコンテンツ削除方法に係る本発明の第３の実施形態を示した図である。

【００７７】この例では、フレーム内の暗号化に用いる時変鍵とは別に、各フレームについても時変鍵を用いて暗号化する。これによりフレーム単位に暗号化を行う場合についても、ＭＯＶＥやＰＡＵＳＥ時に本方式によるコンテンツ削除方式を適用することが出来る。

【００７８】図２４は本発明を用いたコンテンツ削除における鍵の更新方法の一具体例を示す図である。ｔ０、ｔ１…は各処理が行われた時点を示す。

【００７９】タイトル鍵領域を時変鍵で更新する場合、時点ｔ１のように直接上書きする代わりに一時領域に書き込みを行う。その後時点ｔ３のように更新フラグを１に変更する。一時領域はタイトル鍵記憶部１４内に設けられ、更新フラグはタイトル鍵記憶部１４あるいは他の不揮発性メモリ領域に設けられる。次に、ｔ４のようにタイトル鍵領域の鍵を更新し、更新終了後時点ｔ６のように更新フラグを０に戻す。これにより鍵の更新中、障害によりクラッシュした場合、更新フラグが１の場合は一時領域の鍵、更新フラグが０の場合はタイトル鍵領域の鍵を参照することで、クラッシュによる鍵の消失を防ぐことができる。

【００８０】

【発明の効果】以上説明したように本発明によれば、著作権保護機能により保護されたコンテンツをＭＯＶＥ処理もしくはＰＡＵＳＥ処理する際に、元のコンテンツを安全かつ効率的に削除することができる。

【図面の簡単な説明】

【図１】本発明に係るコンテンツ管理装置の構成の一実施形態を示すブロック図。

【図２】コンテンツに付与される著作権保護情報の一例を示す図。

【図３】著作権保護のかかったコンテンツに対するＭＯＶＥ・ＰＡＵＳＥ処理の概要を示す図。

【図４】ＭＯＶＥ処理を具体的に説明する図。

【図５】ＰＡＵＳＥ処理を具体的に説明する図。

【図６】従来におけるコンテンツを削除する第１の方式を示した図。

【図７】従来におけるコンテンツを削除する第２の方式を示した図。

13

【図８】従来におけるコンテンツを削除する第３の方式を示した図。

【図９】本方式におけるコンテンツを削除する方式の概略を示した図。

【図１０】コンテンツ暗号化方式の一例を示す図。

【図１１】図１０で示した暗号化方式により暗号化されたコンテンツを復号化する処理を示した図。

【図１２】本発明に係るコンテンツ復号化の際に行われるコンテンツ削除処理の第１の実施形態について示した図。

【図１３】本方式におけるコンテンツ削除方式を適用した場合のＭＯＶＥ処理において、処理中に障害が発生した場合の動作を示した図。

【図１４】本方式によるコンテンツ削除方式を用いたＭＯＶＥ処理におけるタイトル鍵上書きのタイミングについて示した図。

【図１５】本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第１の具体例について示した図。

【図１６】本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第２の具体例について示した図。

【図１７】本方式によるコンテンツ削除方式を用いたＰＡＵＳＥ処理におけるタイトル鍵上書きのタイミングに関する第３の具体例について示した図。

【図１８】本発明によるコンテンツ削除の第２の実施形態を示した図。

【図１９】本方式によるコンテンツ復号化処理時におけるコンテンツ削除方法を示すフローチャート。

【図２０】本方式によるコンテンツ削除の別の具体例を示した図。

【図２１】図２０で示したコンテンツ削除方式を用いた場合における特殊再生およびサーチの動作を示す図。

【図２２】従来におけるコンテンツ削除方法に関する別の具体例を示す図。

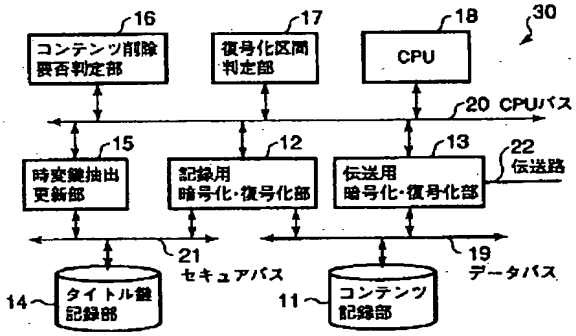
【図２３】図２２のような暗号化が適用された場合におけるコンテンツ削除方法に係る本発明の第３の実施形態を示す図。

【図２４】本発明を用いたコンテンツ削除における鍵の更新方法の一具体例を示す図。

【符号の説明】

１１…コンテンツ記録部、１２…記録用暗号化・復号化部、１３…伝送用暗号化・復号化部、１４…タイトル鍵記録部、１５…時変鍵抽出更新部、１６…コンテンツ削除要否判定部、１７…復号化区間判定部、１８…ＣＰＵ、３０…コンテンツ管理装置

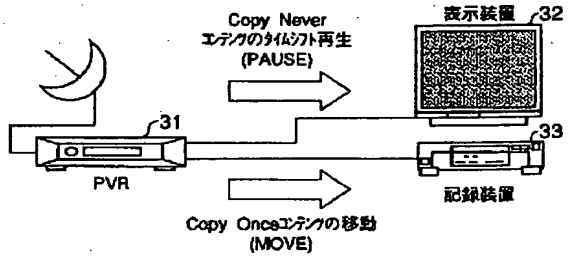
【図１】



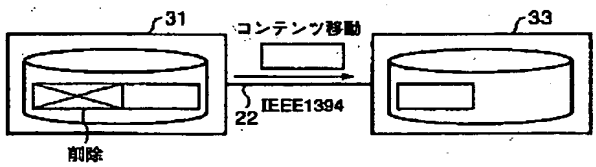
【図２】

データ	定義
00	Copy Free
01	No More Copy
10	Copy Once
11	Copy Never

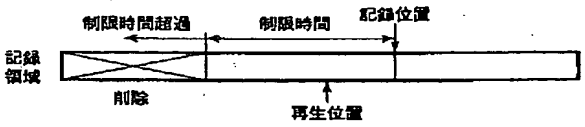
【図３】



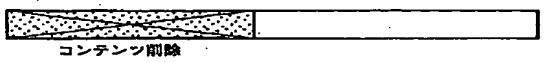
【図４】



【図５】

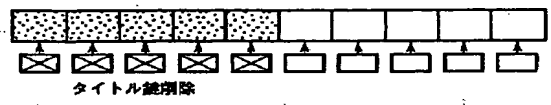


【図６】

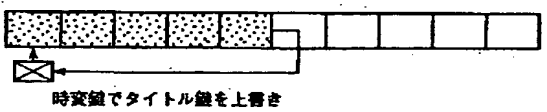


【図７】

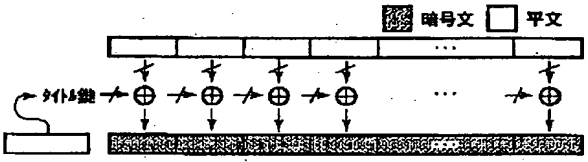
【図８】



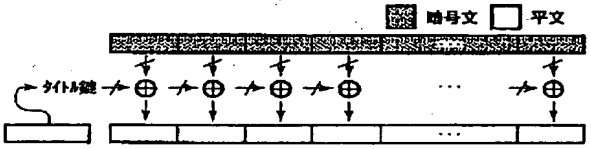
【図９】



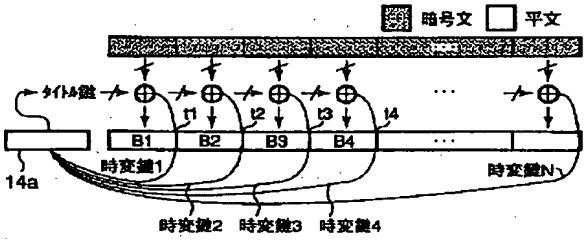
【図１０】



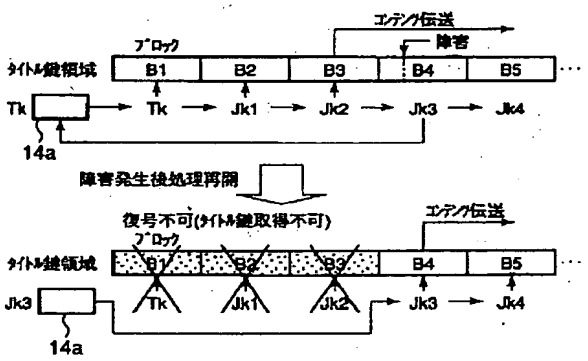
【図１１】



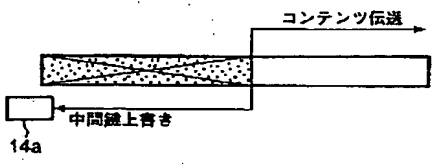
【図１２】



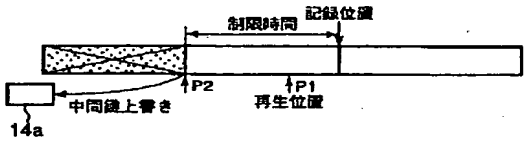
【図１３】



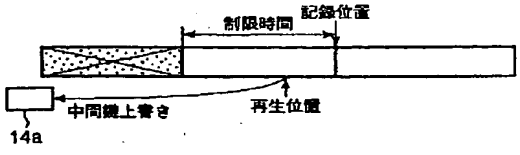
【図１４】



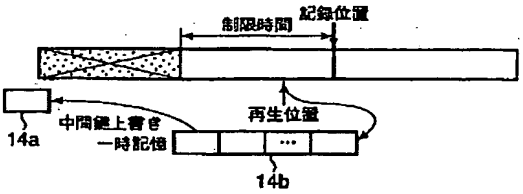
【図１５】



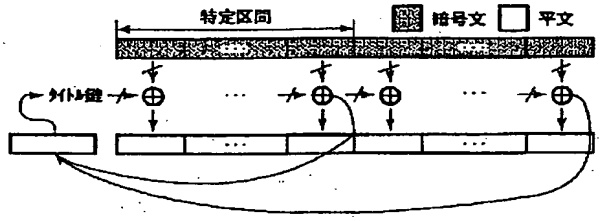
【図１７】



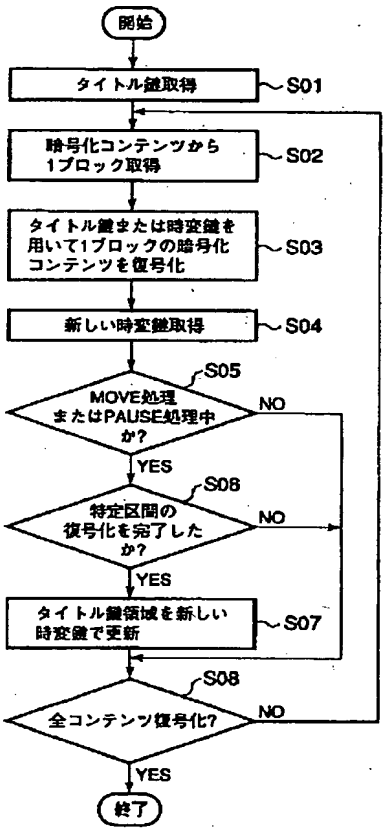
【図１６】



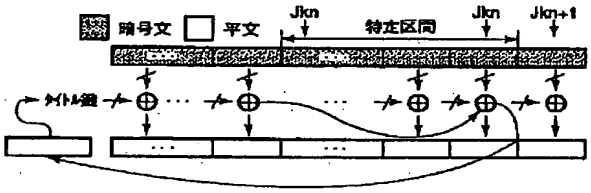
【図１８】



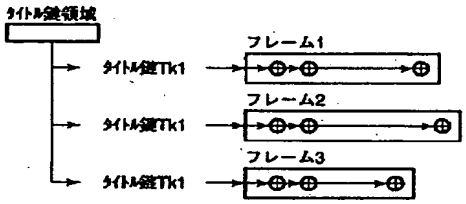
【図１９】



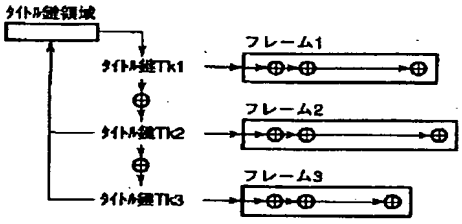
【図２０】



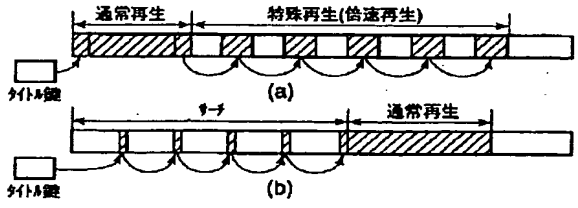
【図２２】



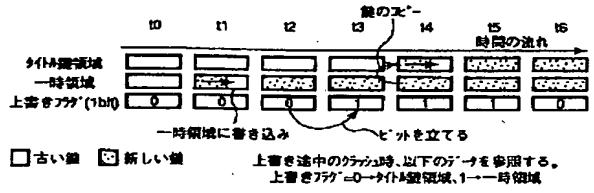
【図２３】



【図２１】



【図２４】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I			テーマコード（参考）
Ｈ０４Ｎ	5/765	Ｈ０４Ｌ	9/00	６４３	５Ｄ０４４
	5/91	Ｈ０４Ｎ	5/91	Ｐ	５Ｊ１０４
	5/92			Ｌ	
	5/93		5/92	Ｈ	
	7/08		5/93	Ｅ	
	7/081		7/08	Ｚ	
	7/167		7/167	Ｚ	
	7/173 ６３０				

Ｆターム（参考） 5B017 AA07 BA07 CA16
5C052 AA01 AB03 AC05 CC06 CC11 DD04
5C053 FA13 FA20 FA21 FA23 GA11 GB06 GB37 HA24 JA21 KA24 LA06 LA07 LA15
5C063 AA01 AB03 AB05 AC01 AC05 AC10 CA11 CA23 CA36 DA07 DA13 DB10
5C064 BA01 BB02 BC06 BC17 BC18 BC22 BC23 BC25 BD02 BD08 BD09 BD13 CA14 CB01 CC04
5D044 AB05 AB07 BC01 BC04 CC04 DE17 DE50 EF05 FG18 GK17 HL08
5J104 AA01 AA34 NA02